

GAO

Testimony

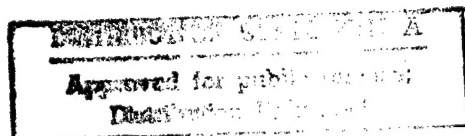
Before the Subcommittee on Technology
Committee on Science
House of Representatives

For Release on Delivery
Expected at
10 a.m.
Thursday,
August 6, 1998

FAA SYSTEMS

Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division



19980819 065

Ms. Chairwoman and Members of the Subcommittee:

We appreciate the opportunity to update the Subcommittee on significant information technology challenges confronting the Federal Aviation Administration (FAA)—challenges that affect the level of risk facing the agency and the flying public. My statement today will focus on two critical issues: the Year 2000 computing crisis and computer security. It will also address the need to correct underlying weaknesses in FAA's management that have allowed these and other key information technology problems to persist. In doing so I will report on actions taken by FAA in response to our recommendations on the Year 2000 problem and computer security,¹ the risks that remain on both of these issues, and FAA's efforts to address our recommendations to improve the way it manages information technology.

In brief, FAA has made progress in managing its Year 2000 problem and has completed critical steps in defining which systems need to be fixed and how to fix them. However, with less than 17 months to go, FAA must still correct, test, and implement many of its mission-critical systems. It is doubtful that FAA can adequately do all of this in the time remaining. Accordingly, it must determine how to ensure continuity of critical operations in the likely event of some systems' failures.

Turning to computer security, FAA cannot provide assurance that the air traffic control systems on which it depends are sufficiently resistant to intrusion. FAA's weak computer security practices were detailed in the classified version of a report we made available in May to key congressional committees and appropriate agency officials. An unclassified version of the report is available to the public.²

Underlying weaknesses in FAA's management have allowed the agency's Year 2000, computer security, and other information technology problems to persist. Our work over the last 2 years has identified some of the root causes of, and pinpointed solutions to, these long-standing problems—including an incomplete systems architecture, weak software acquisition capabilities, unreliable cost information, and a problematic organizational culture. Although FAA has initiated efforts in response to some of our recommendations on these issues, most of them have not been fully implemented.

¹See FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically (GAO/AIMD-98-45, January 30, 1998) and Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety [unclassified version] (GAO/AIMD-98-155, May 18, 1998).

²GAO/AIMD-98-155, May 18, 1998.

Year 2000: Serious Challenges Remain Unresolved

To perform its mission, FAA is dependent on an extensive array of information processing and communications technologies. Without these specialized systems, the agency cannot effectively control air traffic, target airlines for inspection, or provide up-to-date weather information to pilots and air traffic controllers. For example, each of FAA's 20 en route air traffic control facilities, which monitor aircraft at the higher altitudes between airports, depends on about 50 interrelated computer systems to safely guide and direct aircraft. The implications of FAA's not meeting the Year 2000 deadline are enormous, and could affect hundreds of thousands of people—through customer inconvenience, increased airline costs, grounded or delayed flights, or degraded levels of safety.

In testimony this February before this Subcommittee and the Subcommittee on Government Management, Information and Technology, House Committee on Government Reform and Oversight, we stated that FAA was running out of time in making its systems ready for the Year 2000.³

We warned that systems that support critical FAA operations—such as monitoring and controlling air traffic and targeting airline inspections—could fail to perform as needed unless proper date-related calculations could be assured.

At that time, FAA was severely behind schedule in implementing an effective Year 2000 program. In fact, it had no Year 2000 program manager or plan. It had not completed a systems inventory, assessment of its systems for date dependencies, final plans for addressing any such dependencies, or contingency plans for continued operation in case systems were not corrected and implemented in time. As a result, FAA could not judge whether its systems would operate effectively using dates beyond 1999.

Our January 1998 report and February testimony discussed ways in which FAA could mitigate its risk of Year 2000 complications by utilizing a structured approach and rigorous program management.⁴ We made a series of recommendations aimed at assisting FAA in completing overdue

³Year 2000 Computing Crisis: FAA Must Act Quickly to Prevent Systems Failures (GAO/T-AIMD-98-63, February 4, 1998).

⁴One generally accepted approach, outlined in our Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14), includes five phases: (1) the awareness phase entails defining the problem and gaining executive-level support, (2) the assessment phase involves inventorying and analyzing systems, and prioritizing their conversion or replacement, (3) the renovation phase deals with converting, replacing, or eliminating selected systems, (4) the validation phase entails testing and validating that all converted or replaced systems and interfaces will work in an operational environment, and (5) the implementation phase entails deploying and implementing Year 2000-compliant systems and components, and implementing contingency plans, if necessary.

awareness and assessment activities, among them (1) completing an agencywide plan that provides the FAA Year 2000 program manager with the authority to enforce policy, and outlines the agency's overall strategy, (2) assessing how the major FAA components and the aviation industry would be affected if Year 2000 problems were not corrected in time, (3) ranking activities according to level of importance and obtaining and publicizing management commitment and support for Year 2000 initiatives, (4) completing inventories of all information systems and their components, including data interfaces, (5) completing assessments of all systems to determine each one's criticality and to decide whether each system should be converted, replaced, or retired, (6) determining priorities for systems conversion on the basis of mission criticality, (7) developing test and validation plans for converted or replaced systems, and (8) formulating contingency plans to ensure continuity of critical operations.

Officials of both FAA and the Department of Transportation (DOT) agreed with these recommendations, and the agency has made progress in implementing them. A Year 2000 program manager now reports directly to the Administrator and oversees a program plan with specific goals and milestones. Further, FAA has prioritized its systems conversion efforts—an essential step—and developed a master schedule defining which systems will be converted first. The agency has also drafted an end-to-end testing strategy, and is using our business continuity and contingency planning guide⁵ to develop a National Airspace System business continuity and contingency plan. FAA intends to issue this plan in late August.

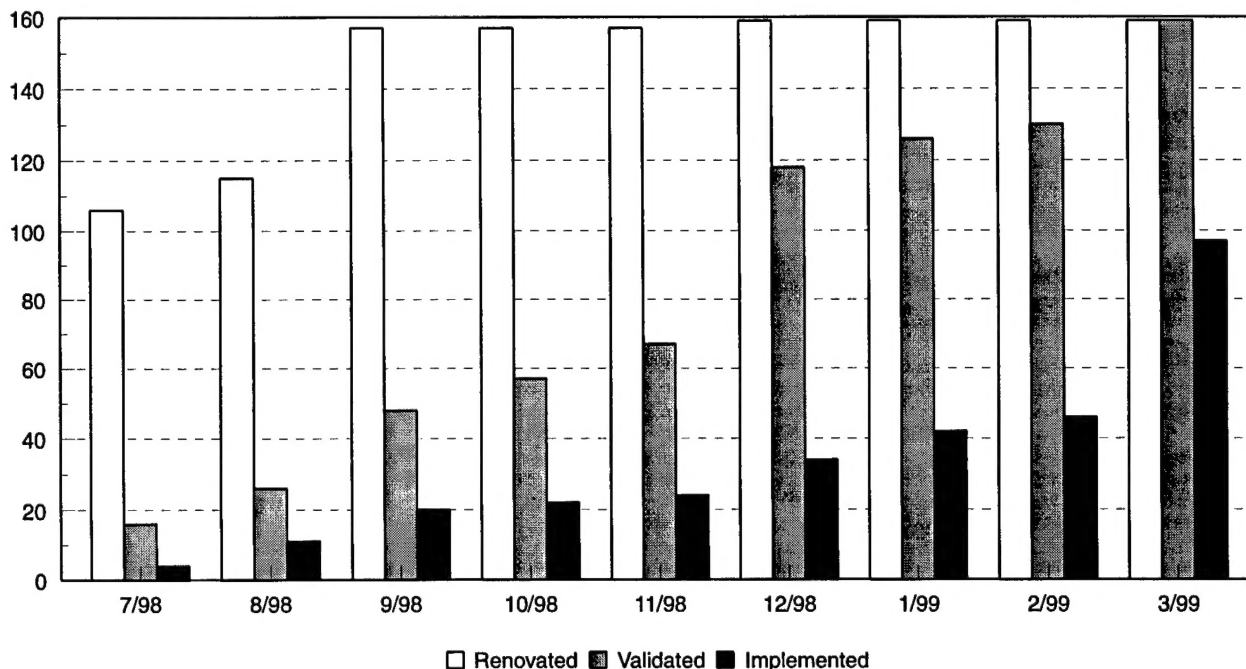
FAA Reports Progress, but It Is Unlikely to Complete Critical Testing Activities in Time

On July 31, FAA announced that 67 percent of its mission-critical systems in need of repair were renovated, exceeding its goal of 60 percent. However, FAA's July 31 projections for completing renovation, validation, and implementation of the 159 mission-critical systems it is repairing will not meet the Office of Management and Budget's (OMB) September 1998 and January and March 1999 milestones, respectively. In addition to these 159 systems, another 44 systems are being replaced. Of these, 38 are not scheduled to be replaced until June 30, 1999, according to FAA's schedules. These replacement systems, too, must be validated and implemented. FAA Year 2000 program officials stated that these replacement dates may not be accurate and that they will be reassessing them in the near future.

⁵Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, August 1998).

Figure 1: Planned Pace of FAA's Mission-Critical Systems Renovation, Validation, and Implementation

Number of systems renovated/validated/implemented (out of 159 to be repaired)



Source: FAA, July 31, 1998.

As figure 1 shows, while FAA projects that 99 percent (157 systems) of the 159 systems will meet OMB's renovation deadline of September 30, 1998, it expects only 79 percent (126 systems) to meet the January 1999 validation deadline, and just 61 percent (97 systems) to meet the March 1999 implementation deadline. FAA plans to complete implementation by June 30, 1999.

Moreover, these projections are based on very optimistic schedules that may not prove to be realistic. One reason is that officials are counting on a steep rise in the pace of completion activity. For example, currently 106 of the 159 systems have been renovated, 9 more are set to be renovated by the end of this month, and a total of 157 by September of this year; this means that 42 systems will have to complete renovation within 1 month.

Validation and implementation also show ambitious schedules. As of July 31, sixteen systems had been validated; by November, that number is set to be 67; by December, 118; and by next January, 126. Finally, as of July 31, just 4 systems out of 159 had been implemented. FAA projects that this number will climb to 46 by next February and, 1 month later—in March 1999—reach 97. According to the Year 2000 program manager, FAA is now reassessing its schedule.

Another reason for uncertainty about FAA's projected milestones is that, according to the Year 2000 program manager, after solutions are tested and validated at FAA's technical centers (scheduled to be completed by March 31, 1999), many must then be tested and implemented at scores of field sites across the country. A task of this complexity—concurrently rolling out numerous system changes to many sites—will likely be time-consuming and filled with difficult implementation challenges, yet FAA projects full implementation by June 30, 1999—only 3 months later. As a comparison, an FAA official responsible for maintaining the Host Computer System stated that it generally takes 4 to 6 weeks to test and implement a single modification once it has been deployed to the en route centers. Multiple concurrent changes would likely prolong this process.

Further, in addition to field testing individual systems, FAA must test its critical business processes and supporting systems end-to-end. In June we testified that agencies will need a significant amount of time for essential end-to-end testing of multiple systems that have individually been deemed Year 2000 compliant.⁶ Such end-to-end testing seeks to ensure that systems collectively supporting a core business function or area operate as intended.⁷ Without such testing, systems individually deemed compliant may not work as expected when linked with other systems in an operational environment. These systems include not only those owned and managed by the organization, but also any external systems with which they interface.

FAA's Year 2000 repair process incorporates an end-to-end test program. However, FAA's draft end-to-end test program plan is not sufficiently detailed to provide an understanding of how the agency plans to accomplish this testing. For example, many of the test threads (paths) have not yet been determined, meaning that FAA does not yet know what specific end-to-end tests it will run or what systems will be included in the

⁶Year 2000 Computing Crisis: Actions Must Be Taken Now to Address Slow Pace of Federal Progress (GAO/T-AIMD-98-205, June 10, 1998).

⁷Year 2000 Computing Crisis: A Testing Guide, Exposure Draft (GAO/AIMD-98-10.1.21, June 1998).

tests. Some of the test threads that have not yet been determined include the descriptions and data flows for en route systems, airport towers, and weather information. This means that FAA has not yet designed the end-to-end tests needed to demonstrate that high altitude air traffic, as well as takeoffs and landings, can be effectively controlled, and that pilots can be effectively alerted to changes in weather conditions. Data interfaces both internal to FAA and involving external parties will also be crucial to this testing. FAA intends to complete its end-to-end testing plan by August 30.

FAA Has Not Yet Resolved Crosscutting Risks That Threaten Aviation Operations

In addition to the risks identified above, FAA must mitigate other critical, crosscutting risks that threaten aviation operations. These include managing the renovation and testing of data exchanges, coordinating with international partners, relying on others for telecommunications support, and planning for business continuity and contingencies.

Significant Risks Persist: Data Exchanges

Examination of data exchanges is essential to every Year 2000 program. Even if an agency's—or company's—internal systems are Year 2000 compliant, unless external entities with which data are exchanged are likewise compliant, critical systems may fail. The first step is to inventory all data exchanges. Exchange partners, once inventoried, must be contacted; agreements must be reached as to what corrections must be made, by whom, and on what schedule; and requisite testing must be defined and performed to ensure that the corrections do, in fact, work.

FAA is not managing this effort effectively. OMB instructed agencies to inventory all external data exchanges by February 1 of this year and coordinate with these exchange partners by March 1. However, as of July 31 FAA's Year 2000 program office still had not completed its inventory. Though incomplete, FAA's data exchange inventory currently lists 1,386 interfaces, of which 361 exchange date-related data and 341 do not. FAA does not yet know if the remaining 684 interfaces—most of which involve air traffic control systems—exchange date-related data. Of the 361 interfaces that are known to exchange such data, FAA has identified 333 that need repair.

Further, FAA does not know how many exchange partners have been contacted, how many agreements have been reached, what these agreements are, or which of them are being implemented. Without this critical information, FAA is not in a position to effectively manage interface

corrections—which could delay the agency’s ability to run critical end-to-end tests and subsequently impair mission-critical operations in the year 2000. For example, the Enhanced Traffic Management System (ETMS) is a mission-critical system that links FAA to airports, airlines, and the weather service, and is integral to managing traffic flow throughout the country. At present, the Year 2000 program office does not know if some party has taken responsibility for fixing each of ETMS’ interfaces, or whether this repair is underway. Without this assurance, FAA may not be able to complete end-to-end testing as planned, thus risking its ability to adequately manage air traffic flow across the nation into the year 2000.

A Year 2000 program official stated that FAA expects to have all agreements with external exchange partners in place when system-specific test plans are completed on September 30, 1998. Because of the vast amount of information that is still not known about data exchanges and the amount of data that would be needed to reach sound agreements (including data formats, test strategies, and time frames), we believe that this expectation is unrealistic. FAA’s Year 2000 program manager recently stated that he planned to reevaluate this schedule.

Significant Risks Persist: International Coordination

American international carriers operate in over 90 countries and at over 200 foreign airports; similarly, over 125 foreign carriers cross FAA-controlled airspace. While FAA lacks the authority and resources to ensure compliance of any foreign air traffic control system, it nevertheless retains responsibility for ensuring safe, reliable aviation services for American travelers into 2000 and beyond. This includes coordination with countries through whose airspace we fly, as well as with those in which we land.

The President has ordered executive agencies to “communicate with their foreign counterparts to raise awareness of and generate cooperative international arrangements to address the [Year 2000] problem.”⁸ In response to this mandate, FAA is working with the International Civil Aviation Organization, which has regulatory responsibility and authority for international aviation safety. Together with the International Air Transport Association and the United Kingdom, they have established the Informal Global Y2K (Year 2000) Coordination Action Group, which meets monthly in Montreal, Canada.

⁸Executive Order 13073, February 4, 1998.

According to FAA's Year 2000 Special Projects Manager, responsible for international coordination, FAA has informal information on the Year 2000 status of 21 of the 90 nations to which U.S. carriers fly, and plans to contact the others to obtain status information in coming months. As detailed in the prior section on data exchanges, FAA must also reach agreements with foreign countries as to the party responsible for renovating interfaces, and how testing will be accomplished. To date, FAA has identified 175 interfaces with 27 countries, but does not know how many of these interfaces must be renovated, by whom, or according to what schedule.

Other international issues that must be addressed include confirming the Year 2000 compliance status of foreign air traffic control (ATC) systems, aircraft, airport infrastructures (including security systems), the systems of suppliers to air carrier and business operations, and contingency planning. According to a Year 2000 program official, FAA plans to work with the global coordination group to address these issues. However, schedules for completing these activities have not yet been developed.

Significant Risks Persist: Reliance on the Telecommunications Infrastructure

In June 16, 1998, testimony, we reported that the Year 2000 readiness of the telecommunications sector is one of the most crucial concerns to our nation because telecommunications is critical to the operations of nearly every public- and private-sector organization.⁹ Reliable telecommunications services are made possible by a complex web of highly interconnected networks supported by national and local carriers and service providers, equipment manufacturers and suppliers, and customers. The key is interoperability: all of the pieces must work together.

FAA relies heavily on both owned and leased telecommunications equipment and services. Whereas FAA is responsible for correcting all of the telecommunications systems it owns, it relies on others to correct its leased equipment and services. FAA advised its vendors of leased equipment and services of their contractual responsibilities to ensure that their systems and services would be Year 2000 compliant. Where necessary, FAA modified contracts to add specific language to this effect. Additionally, FAA reported that it is working in partnership with its telecommunications contractors to ensure that systems are repaired and tested. However, in its May 15, 1998, quarterly Year 2000 report to OMB, DOT

⁹Year 2000 Computing Crisis: Telecommunications Readiness Critical, Yet Overall Status Largely Unknown (GAO/T-AIMD-98-212, June 16, 1998).

reported that even with this level of cooperation, third-party vendors and suppliers may fail to ensure compliance—which could have a significant impact on renovation, testing, and implementation schedules. If such a scenario were to occur, FAA operations that are critically dependent on leased telecommunications—including air traffic control—risk not being renovated in time, further emphasizing the need for effective and tested continuity and contingency plans.

Significant Risks Persist: Business Continuity and Contingency Planning

Business continuity and contingency planning for the year 2000 is critical. Today we are releasing in final form our guidance on this issue, which has been available as an exposure draft since March.¹⁰ OMB has adopted this guidance as the standard that federal agencies are to use in developing their business continuity and contingency plans.

FAA requires contingency plans for each system being repaired or replaced; some of these plans are currently being assessed by an FAA contractor. In addition, FAA is preparing a National Airspace System continuity plan to ensure that critical operations continue should these mission-critical systems fail.

The National Air Traffic Controllers' Association (NATCA) recently expressed concerns about FAA's contingency planning, stating that contingency plans for certain FAA facilities do not adequately define the role of air traffic controllers. NATCA officials explained that should some "worst case" Year 2000 scenarios occur—such as a critical facility's losing all power—FAA contingency plans require surrounding facilities to take over the air traffic control responsibilities of the failed facility. However, the contingency plans do not specify how the surrounding facilities would assume or perform these responsibilities. For instance, it is not clear which controllers would pick up which sectors of airspace, or even what information (speed, altitude, location, heading) would be available to them. Should worst-case scenarios occur, this lack of critical information could degrade aircraft safety.

We are currently reviewing FAA's continuity and contingency plans at the request of the House Appropriations Subcommittee on Transportation.

¹⁰Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, August 1998).

FAA Reports That the Critical Host Computer System Is Renovated, but Testing Is Not Yet Complete

The Host Computer System is FAA's key information processing system for its 20 en route centers, which control aircraft in transit over the continental United States and during approaches to some airports. It processes radar surveillance data and flight plans, links filed flight plans with actual aircraft flight tracks, provides alerts of projected aircraft separation violations, and processes weather data.

As we reported this May, FAA plans to replace the Host system by October 1999 for two key reasons.¹¹ First, the Host is approaching the end of its useful life. Host hardware was installed at the 20 en route centers between 1986 and 1988, with an expected service life of 10 years. Now past that time, critical spare parts are in short supply. It is estimated that the inventory of one critical spare part in particular, the CLVM,¹² will be depleted in 1999. Once these parts are gone, FAA plans to cannibalize parts from Host systems in its training and technical support centers. Even with cannibalization, however, FAA states that the Host cannot be maintained beyond 2001.

The second reason for replacing the Host is that its manufacturer, IBM, has stated that it has no confidence in the system's ability to survive the century date change because IBM no longer employs people with the skills necessary for assessing the Host processor's microcode (low-level machine instructions used to service the IBM 3083 mainframe).

As a back-up plan to replacing the Host, FAA decided to renovate the microcode. FAA announced in late July that it had successfully renovated and was in the process of testing the Host system. To do so, FAA hired retired workers familiar with the microcode, and tested all components using specially developed microcode diagnostic tools. FAA's renovation and testing efforts thus far appear reasonable. However, FAA cannot be confident that the Host will support critical operations—should the Host replacement not be deployed to all 20 en route centers in time—until after testing, including end-to-end testing, has been completed.

¹¹Air Traffic Control: FAA Plans to Replace Its Host Computer System Because Future Availability Cannot Be Assured (GAO/AIMD-98-138R, May 1, 1998).

¹²According to FAA officials, the meaning of CLVM has been forgotten over time, although it may stand for Cache Link Volatile Memory. Basically, CLVM is the module that provides memory storage for efficient heat dissipation.

Computer Security: Weak Practices Degrade Safety

While poor computer security practices are a pervasive high-risk problem across government,¹³ the risks they pose in the air traffic environment are particularly serious. Failure to adequately protect these systems, as well as the facilities that house them, threatens nationwide disruption of air traffic or even loss of life due to collision.

In assessing the adequacy of computer security at FAA earlier this year, we found significant weaknesses that compromise the integrity of FAA's air traffic control operations.¹⁴ This review resulted in a number of findings too sensitive to discuss in today's open hearing; accordingly, my statement will refer only to findings and recommendations contained in the unclassified version of our limited official use report. We can tell you openly, though, that we found evidence of air traffic control systems that had been penetrated, and critical ATC data that had been compromised.

FAA's ATC network is an enormous collection of interrelated systems that reside at or are associated with hundreds of ATC facilities. The systems and facilities are interconnected by complex communications networks that separately transmit both voice and digital data. While the use of interconnected systems offers significant benefits in improved government operations, it also increases vulnerability to anonymous intruders who may manipulate data to commit fraud, obtain sensitive information, or severely disrupt operations. Since this interconnectivity is expected to grow as ATC systems are modernized to meet the projected increases in air traffic and to replace aging equipment, the ATC network will become even more vulnerable to such network-related threats.

Intruders can use a variety of techniques to attack computer systems. Consequently, it is essential that FAA's approach to computer security be comprehensive and include the following three elements: the physical security of the facilities that house ATC systems (e.g., locks, guards, fences, and surveillance equipment); information security of the systems (e.g., safeguards incorporated into computer hardware and software); and telecommunications security of the networks linking the systems and facilities (e.g., secure gateways, firewalls, and communications-protection devices).

¹³High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

¹⁴GAO/AIMD-98-155, May 18, 1998 and Information Security: Serious Weaknesses Put State Department and FAA Operations at Risk (GAO/T-AIMD-98-170, May 19, 1998).

FAA had significant weaknesses in every area of computer security that we investigated: physical security, operational system security,¹⁵ development of new systems, and FAA's management structure and implementation of computer security policy. I'd like to briefly address each of these areas.

ATC Physical Security Management and Controls Are Ineffective

FAA policy dating to 1993 required airport towers, TRACONs,¹⁶ en route centers, and other facilities to be inspected within 2 years and mandated that following that, annual or triennial inspections be performed, depending on the type of facility. Such inspections were required to determine whether a facility met physical security standards and could, then, be accredited as secure.

The agency's management of physical security at its ATC facilities that control aircraft has been ineffective. Known physical security weaknesses exist at many facilities. For example, an FAA inspection report found 26 physical security findings at one location alone, among them fire protection systems below minimum standards, and contract service employees' being given unrestricted access to sensitive areas. FAA's assessment of another facility concluded that access control procedures were weak to nonexistent, and that the facility was extremely vulnerable to criminal and terrorist attack. Further, we found that FAA was unaware of physical security weaknesses that may exist at other facilities because many have not been inspected. FAA had not assessed physical security controls at 187 facilities since 1993 and, therefore, did not know how vulnerable they are. Until FAA inspects its remaining facilities, it cannot know whether they are secure and if the appropriate controls are in place to prevent loss or damage to FAA property, injury to FAA employees, or compromise of FAA's capability to perform critical air safety functions.

In our May 1998 report,¹⁷ we recommended that the 187 facilities that had not been recently assessed be inspected and accredited as soon as possible, but no later than April 30, 1999; that any identified weaknesses be corrected; and that annual or triennial inspections be carried out, any deficiencies corrected, and accreditation kept current. All of this is required by current FAA policy. On July 22 of this year, FAA officials told us that they had completed inspections of all facilities, but had not yet corrected all identified weaknesses. These officials told us that a plan for

¹⁵This includes both information systems and telecommunications networks.

¹⁶Terminal radar approach control facilities.

¹⁷GAO/AIMD-98-155, May 18, 1998.

correcting the physical security weaknesses that remain is to be completed by August 30, 1998. Until these weaknesses are corrected, many facilities will remain physically vulnerable.

ATC Operational Systems Security Is Ineffective and Systems Are Vulnerable

FAA policy requires that all ATC systems be certified and accredited.¹⁸ A risk assessment, which identifies and evaluates vulnerabilities, is a key requirement for certification and accreditation. As we have reported, leading information security organizations use risk assessments to identify and manage security risks confronting their organizations.¹⁹

FAA has not assessed, certified, or accredited most of its operational ATC systems. According to FAA's latest information, less than 10 percent of its operational systems—7 of 90—have undergone risk assessments. As a result, FAA does not know how vulnerable these operational systems are and consequently has no basis for determining how to best protect them. Further, of the seven assessed systems, only three were granted certification because the proper documentation was lacking for the other four. In addition, FAA has not assessed most ATC telecommunications systems. For example, according to officials responsible for maintaining the nine FAA-owned or -leased communications networks, only one has been assessed. Such poor security management exists despite the fact that FAA's 1994 Telecommunications Strategic Plan stated that "vulnerabilities that can be exploited in aeronautical telecommunications potentially threaten property and public safety." FAA's 1997 Telecommunications Strategic Plan continues to identify security of telecommunications systems as an area in need of improvement.

FAA officials told us that they are not aware of a single ATC system that has been accredited. FAA's Associate Administrator for Civil Aviation Security, who is responsible for accrediting systems, explained that FAA has decided to spend its limited funds on developing new systems rather than securing those currently in operation. He further stated that FAA management is reluctant to acknowledge information security threats.

¹⁸System certification is the technical evaluation that is conducted to verify that FAA systems comply with FAA security requirements, identify security deficiencies, specify remedies, and justify exceptions. Certification results are one factor management considers in deciding whether to accredit systems. Accreditation is the formal declaration from management that the appropriate security safeguards have been properly implemented and that residual risk is acceptable.

¹⁹Executive Guide: Information Security Management: Learning from Leading Organizations (GAO/AIMD-98-68, May 1998).

FAA maintains that opportunities for unauthorized access to its systems are limited by its use of custom-built, 20-year-old equipment having proprietary communications interfaces and custom-built software. This position is not supported. First, the archaic and proprietary features of the ATC system provide no protection from attack by disgruntled current or former employees who understand them. Second, while these configurations may not be commonly understood by external hackers, one cannot conclude that old or obscure systems are, by definition, secure. In fact, the few certification reviews that FAA has done reveal operational systems vulnerabilities.

Given the importance of such systems' security, we recommended that all ATC systems be assessed, certified, and accredited as expeditiously as possible, but no later than April 30, 1999, in accordance with FAA policy, and that all systems likewise undergo these steps every 3 years, as also required.

FAA officials recently told us that they will not be able to assess, certify, and accredit all operational ATC systems by April 30, 1999. However, they said that they have tasked the Volpe National Transportation Center²⁰ with performing risk assessments of some operational systems and developing an overall plan by August 30, 1998, that details which systems will be assessed and when.

FAA Is Not Effectively Incorporating Security Features Into New ATC Systems

Essential computer security measures can be provided most efficiently and cost-effectively if addressed during systems design. In contrast, retrofitting security features into an operational system is far more expensive, and often less effective. Sound overall security guidance—including a security architecture, security concept of operations, and security standards—is needed to ensure that well formulated security requirements are included in specifications for all new ATC systems.

FAA has no security architecture, concept of operations, or standards.²¹ As a result, implementation of security requirements across ATC development is sporadic and ad hoc. Of the six current ATC system development efforts

²⁰The John A. Volpe National Transportation Systems Center, in Cambridge, Massachusetts, is a federal organization whose principal role is transportation and logistics expertise. It provides research, management, and engineering support to DOT, other federal agencies, and state and local governments.

²¹Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization (GAO/AIMD-97-30, February 3, 1997).

that we reviewed, four had security requirements, but only two of the four developed those requirements using risk assessments. Without risk assessments, FAA has no formal analytical basis for its security requirements or design and lacks assurance that future ATC systems will be protected from attack. With no security requirements specified during systems design, any attempt to retrofit such features later will be increasingly costly and technically challenging.

In 1996 the Associate Administrator for Research and Acquisitions established the National Airspace System (NAS) Information Security (NIS) group to develop the requisite security architecture, security concept of operations, and security standards, along with other elements. According to the group's mission need statement, "information security is the FAA mission area with the greatest need for policy, procedural, and technical improvement. Immediate action is called for, to develop and integrate information security into ATC systems throughout their life cycles." FAA has estimated that it will cost about \$183 million to improve ATC information security, and the NIS group has developed an action plan describing proposed improvement activities. However, over 2 years later, no detailed plans or schedules have been developed to accomplish these tasks.

As FAA modernizes and increases interconnectivity among systems, ATC systems will become more vulnerable. Such vulnerabilities are well documented, both in FAA's information security mission need statement and in reports completed by the President's Commission on Critical Infrastructure Protection.²² The commission summary reported that the future ATC architecture appeared to have vulnerabilities, recommending that FAA act immediately to develop, establish, fund, and implement a comprehensive systems security program to protect the modernized ATC system from information-based and other disruptions, intrusions, and attacks. It further recommended that this program be guided by the detailed recommendations made in the NAS vulnerability assessment.

To improve security for future, modernized ATC systems, we recommended that the Secretary of Transportation direct the FAA Administrator to ensure that specifications for all new ATC systems include security requirements based on detailed assessments. Such security requirements would be

²²The President's Commission on Critical Infrastructure Protection (PCCIP) was established in July 1996, through Executive Order 13010, to assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures, including telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government. As a supplement to the transportation assessment, PCCIP conducted a vulnerability assessment of the NAS architecture.

included as a criterion when FAA analyzes new systems for funding under its acquisition management system. We also recommended that the NIS group establish detailed plans and schedules for developing a security architecture, concept of operations, and security standards—and that these plans be implemented. According to FAA officials, they are initiating action to address these recommendations. For example, just last week we received a briefing on FAA's efforts to build security into its future remote monitoring and maintenance system. Overall, FAA has made progress in building security features into this system and the process it used to derive security requirements is reasonable. However, this is only one of many future systems, and not all future development efforts are using a similar approach to address systems security. Additionally, overall guidance still does not exist to ensure that well formulated security requirements are included in specifications for all new ATC systems.

FAA's Management Structure Is Not Effectively Implementing or Enforcing Computer Security Policy

FAA's management structure and implementation of policy for computer security needs to be greatly improved. Security responsibilities are distributed among three organizations, all of which have been remiss in their ATC security duties: the Office of Civil Aviation Security has not adequately enforced the security policies it has formulated; the Office of Air Traffic Services has not adequately implemented security policy for operational ATC systems; and the Office of Research and Acquisitions has not adequately implemented policy for new ATC systems development. Until existing ATC computer security policy is effectively implemented and enforced, operational and developmental ATC systems will continue to be vulnerable to compromise of sensitive information and interruption of critical services.

While FAA has established a central security focal point in the NIS group, to be effective, this group must have the authority to enforce the organization's security policies, or have access to senior executives who are organizationally positioned to take action and effect change across divisions. Although the NIS group has access to certain key associate administrators, it does not have access to the management level that can effect change across organizational divisions (e.g., FAA's Administrator and Deputy Administrator). One approach for ensuring that a central group have such access at FAA would be to place it under a Chief Information Officer (CIO) reporting directly to the FAA Administrator. We recommended that FAA do so in our May 1998 report.

Problems Persist Because FAA's Management of Its Information Technology Is Ineffective

The initial DOT response to our draft report was disappointing. It discussed FAA's actions for timely correction pertaining to just 1 of our 15 specific recommendations. This lack of commitment was particularly troubling, considering that several of the recommendations simply requested that FAA adhere to its own computer security policies.

When we met with FAA officials late last month, they acknowledged that major improvements are needed in all areas of its computer security program, and discussed preliminary efforts to address most of our recommendations. However, DOT has yet to provide an official written response as to how it plans to address our recommendations.

FAA's Year 2000 and computer security problems can be added to the long list of issues that have confronted FAA in its management of information technology. FAA's effort to modernize its air traffic control system—beginning in 1981 and comprising over 200 separate projects at an estimated cost of about \$34 billion dollars through the year 2003—has been a huge yet necessary undertaking. It was designed to replace and upgrade the system's aging equipment and facilities to meet the anticipated increase in traffic, enhance the margin of safety, and increase the efficiency of ATC.

However, the modernization program has experienced substantial cost overruns, lengthy schedule delays, and significant performance shortfalls. To illustrate, the former centerpiece of the modernization program—the Advanced Automation System (AAS)—was restructured in 1994 after estimated costs to develop the system tripled from \$2.5 billion to \$7.6 billion, and delays in putting significantly less-than-promised system capabilities into operation were expected to run 8 years or more over original estimates. We calculated that of the \$2.6 billion spent on AAS, \$1.5 billion was wasted.²³ Because of the complexity, cost, and problems that have continued to surround FAA's modernization program, we designated it a high-risk information technology initiative in 1995 and again in 1997.²⁴

Our recent reviews have identified some of the root causes of the modernization's problems, along with solutions:

²³Air Traffic Control: Evolution and Status of FAA's Automation Program (GAO/T-RCED-98-85, March 5, 1998).

²⁴See High-Risk Series: An Overview (GAO/HR-95-1, February 1995) and GAO/HR-97-9, February 1997.

-
- **ATC Systems Architecture Is Incomplete.** FAA has attempted its modernization without a complete systems architecture, or blueprint, to guide development and evolution.²⁵ The result has been unnecessarily higher spending to buy, integrate, and maintain hardware and software. We recommended that FAA develop and enforce a complete systems architecture and implement a management structure for doing so that is similar to the Chief Information Officers provisions of the Clinger-Cohen Act of 1996.
 - **ATC Software Acquisition Capabilities Are Weak.** FAA's processes for acquiring software, the most costly and complex component of ATC systems, are ad hoc, sometimes chaotic, and not repeatable across projects.²⁶ As a result, FAA has been at great risk of not delivering promised software capabilities on time and within budget. Furthermore, FAA lacks an effective approach for improving its software acquisition processes. We recommended that FAA undertake a disciplined effort to improve its software acquisition capabilities and reiterated our recommendation that a CIO organizational structure be established for FAA.
 - **ATC Cost Information Is Unreliable.** FAA has neither the cost estimating processes nor the disciplined cost accounting practices it needs to effectively manage its information technology investments. As a result, it is at risk of making ill-informed decisions on critical multimillion-dollar, even billion-dollar air traffic control systems.²⁷ We recommended that FAA institutionalize defined processes for estimating project cost, and develop and implement a managerial cost accounting capability.
 - **FAA's Organizational Culture Is Problematic.** FAA's organizational culture has not reflected a strong commitment to mission focus, accountability, coordination, and adaptability.²⁸ We have recommended that FAA develop a comprehensive strategy for addressing this issue.

FAA has begun to implement many of our recommendations. Specifically, FAA initiated activities to develop a complete ATC systems architecture, to improve its software acquisition capabilities, to institutionalize defined cost estimating processes, and to acquire a cost accounting system. Additionally, FAA issued a strategy for improving its organizational culture,

²⁵GAO/AIMD-97-30, February 3, 1997.

²⁶Air Traffic Control: Immature Software Acquisition Processes Increase FAA System Acquisition Risks (GAO/AIMD-97-47, March 21, 1997).

²⁷Air Traffic Control: Improved Cost Information Needed to Make Billion Dollar Modernization Investment Decisions (GAO/AIMD-97-20, January 22, 1997).

²⁸Aviation Acquisition: A Comprehensive Strategy Is Needed for Cultural Change at FAA (GAO/RCED-96-159, August 22, 1996).

although actual cultural change takes time. Success will depend upon whether FAA sustains its commitment to such change.

FAA initially disagreed with our recommendation to establish a management structure similar to the Department-level CIO prescribed in the Clinger Cohen Act, but recently told us that the Administrator is in the process of hiring a CIO who will report directly to her, and who will be responsible for information management issues, including security. Such a change is needed if FAA is to solve its long-standing information technology management problems.

In summary, FAA faces significant challenges—both in addressing the Year 2000 problem and correcting its computer security weaknesses. Failure to address either of these issues effectively could prove devastating. Careful attention to security issues is even more important during the next 17 months as FAA makes a tremendous number of Year 2000-related changes to its mission-critical systems. If insufficient attention is paid to computer security during this time, existing vulnerabilities will be compounded. In these areas, as in the information technology areas we have reported on over the past few years, strong leadership and rigorous process discipline are needed if FAA is to successfully and safely navigate into the next century.

This concludes my statement. I would be happy to respond to any questions that you or other members of the Subcommittee may have at this time.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are \$2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

<http://www.gao.gov>